Today we are going to study the abstract properties of binary operations.
In how many different ways can we put the square back on the frame?

We will now study these 8 motions, called symmetries of the square:

$$Y_{SQ} = \{ R_0, R_{90}, R_{180}, R_{270}, F_\|, F_-, F_\/, F_\\}$$

**Composition**

Define the operation “•” to mean “first do one symmetry, and then do the next”

For example,

- $$R_{90} \cdot R_{180}$$ means “first rotate 90° clockwise and then 180°”
  - = $$R_{270}$$

- $$F_\| \cdot R_{90}$$ means “first flip horizontally and then rotate 90°”
  - = $$F_\\$$

**Question:** if $$a, b \in Y_{SQ}$$, does $$a \cdot b \in Y_{SQ}$$? Yes!
Some Formalism

If S is a set, \( S \times S \) is:

the set of all (ordered) pairs of elements of S

\( S \times S = \{ (a,b) \mid a \in S \text{ and } b \in S \} \)

If S has \( n \) elements, how many elements does \( S \times S \) have? \( n^2 \)

Formally, \( \ast \) is a function from \( Y_{SQ} \times Y_{SQ} \) to \( Y_{SQ} \)

\[ \ast : Y_{SQ} \times Y_{SQ} \rightarrow Y_{SQ} \]

As shorthand, we write \( \ast(a,b) \) as “\( a \ast b \)”

Binary Operations

“\( \ast \)” is called a binary operation on \( Y_{SQ} \)

Definition: A binary operation on a set \( S \) is a function \( \ast : S \times S \rightarrow S \)

Example:

The function \( f : N \times N \rightarrow N \) defined by

\[ f(x,y) = xy + y \]

is a binary operation on \( N \)

Associativity

A binary operation \( \ast \) on a set \( S \) is associative if:

\[
\text{for all } a,b,c \in S, \quad (a \ast b) \ast c = a \ast (b \ast c)
\]

Examples:

Is \( f : N \times N \rightarrow N \) defined by \( f(x,y) = xy + y \) associative?

\[ (ab + b)c + c = a(bc + c) + (bc + c)? \text{ NO!} \]

Is the operation \( \ast \) on the set of symmetries of the square associative? \text{ YES!}

Commutativity

A binary operation \( \ast \) on a set \( S \) is commutative if

\[
\text{For all } a,b \in S, \quad a \ast b = b \ast a
\]

Is the operation \( \ast \) on the set of symmetries of the square commutative? \text{ NO!}

\[ R_{90} \ast F_1 \neq F_1 \ast R_{90} \]
**Identities**

- $R_0$ is like a null motion
- Is this true: $\forall a \in Y_{SQ}, \ a \cdot R_0 = R_0 \cdot a = a$? YES!
- $R_0$ is called the identity of $\cdot$ on $Y_{SQ}$

In general, for any binary operation $\cdot$ on a set $S$, an element $e \in S$ such that for all $a \in S$, $e \cdot a = a \cdot e = a$ is called an identity of $\cdot$ on $S$

**Inverses**

- Definition: The inverse of an element $a \in Y_{SQ}$ is an element $b$ such that:
  
  $$a \cdot b = b \cdot a = R_0$$

- Examples:
  - $R_{90}$ inverse: $R_{270}$
  - $R_{180}$ inverse: $R_{180}$
  - $F_{\|}$ inverse: $F_{\|}$

Every element in $Y_{SQ}$ has a unique inverse
### Groups

A group $G$ is a pair $(S, \bullet)$, where $S$ is a set and $\bullet$ is a binary operation on $S$ such that:

1. $\bullet$ is associative
2. (Identity) There exists an element $e \in S$ such that: $e \bullet a = a \bullet e = a$, for all $a \in S$
3. (Inverses) For every $a \in S$ there is $b \in S$ such that: $a \bullet b = b \bullet a = e$

If $\bullet$ is commutative, then $G$ is called a commutative group.

### Examples

<table>
<thead>
<tr>
<th>Is $(\mathbb{N}, +)$ a group?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is $+$ associative on $\mathbb{N}$?</td>
</tr>
<tr>
<td>Is there an identity?</td>
</tr>
<tr>
<td>Does every element have an inverse?</td>
</tr>
</tbody>
</table>

$(\mathbb{N}, +)$ is NOT a group

<table>
<thead>
<tr>
<th>Is $(\mathbb{Z}, +)$ a group?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is $+$ associative on $\mathbb{Z}$?</td>
</tr>
<tr>
<td>Is there an identity?</td>
</tr>
<tr>
<td>Does every element have an inverse?</td>
</tr>
</tbody>
</table>

$(\mathbb{Z}, +)$ is a group

<table>
<thead>
<tr>
<th>Is $(\mathbb{Y}_{SQ}, \bullet)$ a group?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is $\bullet$ associative on $\mathbb{Y}_{SQ}$?</td>
</tr>
<tr>
<td>Is there an identity?</td>
</tr>
<tr>
<td>Does every element have an inverse?</td>
</tr>
</tbody>
</table>

$(\mathbb{Y}_{SQ}, \bullet)$ is a group
Examples

Is \((\mathbb{Z}_n, +)\) a group?
\((\mathbb{Z}_n\) is the set of integers modulo \(n)\)

- Is + associative on \(\mathbb{Z}_n\)? YES!
- Is there an identity? YES: 0
- Does every element have an inverse? YES!

\((\mathbb{Z}_n, +)\) is a group

Identity Is Unique

Theorem: A group has at most one identity element

Proof:
Suppose \(e\) and \(f\) are both identities of \(G=(S, \cdot)\)

Then \(f = e \cdot f = e\)

Inverses Are Unique

Theorem: Every element in a group has a unique inverse

Proof:
Suppose \(b\) and \(c\) are both inverses of \(a\)

Then \(b = b \cdot e = b \cdot (a \cdot c) = (b \cdot a) \cdot c = c\)

A group \(G=(S, \cdot)\) is finite if \(S\) is a finite set

Define \(|G| = |S|\) to be the order of the group (i.e. the number of elements in the group)

What is the group with the least number of elements?
\(G = \{(e, \cdot)\}\) where \(e \cdot e = e\)

How many groups of order 2 are there?

\[
\begin{array}{ccc}
e & f \\
e & e & f \\
f & f & e
\end{array}
\]
Generators

A set $T \subseteq S$ is said to generate the group $G = (S, \ast)$ if every element of $S$ can be expressed as a finite product of elements in $T$.

Question: Does $\{R_{90}\}$ generate $Y_{SQ}$? NO!

Question: Does $\{F_i, R_{90}\}$ generate $Y_{SQ}$? YES!

An element $g \in S$ is called a generator of $G = (S, \ast)$ if $\{g\}$ generates $G$.

Does $Y_{SQ}$ have a generator? NO!

Generators For $(\mathbb{Z}_n, +)$

Any $a \in \mathbb{Z}_n$ such that $\text{GCD}(a,n)=1$ generates $(\mathbb{Z}_n, +)$.

Claim: If $\text{GCD}(a,n) = 1$, then the numbers $a, 2a, \ldots, (n-1)a, na$ are all distinct modulo $n$.

Proof (by contradiction):

Suppose $xa = ya \pmod{n}$ for $x, y \in \{1, \ldots, n\}$ and $x \neq y$.

Then $n \mid (x-y)$.

Since $\text{GCD}(a,n) = 1$, then $n \mid (x-y)$, which cannot happen.

Orders

Theorem: Let $x$ be an element of $G$. The order of $x$ divides the order of $G$.

Corollary: If $p$ is prime, $a^{p-1} = 1 \pmod{p}$.

(This is called Fermat’s Little Theorem)

$\{1, \ldots, p-1\}$ is a group under multiplication modulo $p$.

If $G = (S, \ast)$, we use $a^n$ denote $(a \ast a \ast \cdots \ast a)$ $n$ times.

Definition: The order of an element $a$ of $G$ is the smallest positive integer $n$ such that $a^n = e$.

The order of an element can be infinite!

Example: The order of 1 in the group $(\mathbb{Z}, +)$ is infinite.

What is the order of $F_i$ in $Y_{SQ}$? 2

What is the order of $R_{90}$ in $Y_{SQ}$? 4
We can define more than one operation on a set. For example, in $\mathbb{Z}_n$ we can do addition and multiplication modulo $n$. A ring is a set together with two operations.

**Definition:**
A ring $R$ is a set together with two binary operations $+$ and $\times$, satisfying the following properties:
1. $(R,+)$ is a commutative group
2. $\times$ is associative
3. The distributive laws hold in $R$:
   $$(a + b) \times c = (a \times c) + (b \times c)$$
   $$a \times (b + c) = (a \times b) + (a \times c)$$

**Fields**
Definition:
A field $F$ is a set together with two binary operations $+$ and $\times$, satisfying the following properties:
1. $(F,+) \text{ is a commutative group}$
2. $(F - \{0\},\times) \text{ is a commutative group}$
3. The distributive law holds in $F$:
   $$(a + b) \times c = (a \times c) + (b \times c)$$

**In The End...**
Why should I care about any of this? Groups, Rings and Fields are examples of the principle of abstraction: the particulars of the objects are abstracted into a few simple properties. All the results carry over to any group.
Symmetries of the Square
Compositions

Groups
Binary Operation
Identity and Inverses
Basic Facts: Inverses Are Unique
Generators

Rings and Fields
Definition

Here's What You Need to Know...